6 Короткі повідомлення

УДК 002.6 + 347,777 + 343.50/53 + 35.078 + 342.7

ІНФОРМАЦІЙНА БЕЗПЕКА, ЯК НОВА ПАРАДИГМА НОВОГО КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Віталій Цимбалюк, Владислав Гавловський
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю

Анотація: **Розглядаються питання теорії кримінального та інформаційного права, правової інформатики щодо інформаційної безпеки та захисту інформації в автоматизованих системах.**
Summary: **In the article the questions of the theory of the crime and the information right, legal computer science, information safety and protection of the information in the automized systems are considered.**
Ключові слова: **Інформаційна безпека, право, захист інформації в автоматизованих системах.**

З прийняттям нового Кримінального Кодексу України (далі КК) можна констатувати, що відкривається новий етап розвитку наукової думки у правознавстві щодо проблем інформаційної безпеки. При цьому здійснюється формування нових парадигм – взірців, прикладів для усвідомлення і переусвідомлення їх юридичною громадськістю України, у тому числі науковою.

Загально визнано, що кримінальне право має свою провідну функцію – визначає які суспільні відносини небажані для людини, суспільства, держави, є найбільш небезпечні і набувають соціального статусу злочинів. Тобто кримінальне право визначає, чого не можна робити під загрозою покарання через кримінальні санкції. У зв'язку з цим визначається місце кримінального права – головного права щодо забезпечення охорони суспільних відносин та їх особливого захисту державою. Не випадково у багатьох слов'янських мовах це право називається як уголовне право (тобто головне).

Природно, після прийняття КК він піддається і буде піддаватися глибокому аналізу правознавцями, соціологами та науковцями інших галузей знань. Проте слід віддати подяку, пошану і визнання тим, працею, інтелектом кого була проторена дорога новому кримінальному законодавству України і створено умови розвитку наукової думки. А на різку критику на адресу розробників КК можна відповісти народною мудрістю – у будь-якій справі при бажанні легко можна знайти недоліки, але не будь-яка справа легко без недоліків робиться. Хтось, дивлячись на сонце бачить світло, а хтось – плями.

У подальших роздумах науковій громадськості пропонується погляд на КК з позицій юридичної когнітології – науки про пізнання права, правовідносин у контексті єдності теорії соціальної психології, тектології (теорії організації соціальних систем) і теорії інформації в соціальних системах.

Один з головних постулатів юридичної когнітології можна зазначити наступним чином: "будь-яке формулювання (визначення) поняття має базуватися на категоріях, що викликають адекватну рефлексію у суб'єктів суспільних відносин". Особливо це потрібно при визначенні диспозицій злочинів.

Конструктивний, критичний, системно-комплексний правовий аналіз КК свідчить, що у ньому природно поєднані традиції теорії кримінального права з новаціями, що виникли з розвитком нових суспільних відносин. До останніх можна віднести суспільні інформаційні відносини в умовах інформатизації. Серед новацій КК звернемо увагу на з'ясування змісту і сутності категорії "безпека" та похідної від неї категорії "небезпека", "інформаційна безпека" з точки зору такої нової для вітчизняної науки наукової дисципліни, як теорія організації інформаційної безпеки соціальних систем.

За своєю сутністю, виходячи із змісту ст. 1 КК, завдання його визначається також через категорію "безпека" – "за***безп***ечення". Тобто категорія "небезпека" традиційна для теорії кримінального права і, звичайно, вона неодноразово зустрічається у змісті КК. Наприклад (виділяється автором предмет дослідження), стаття 11 – "Злочином є передбачене цим Кодексом суспільно не***безпечне*** … діяння"…

Виходячи тільки із зазначених прикладів, виникає необхідність визначення категорії "безпека". Кримінальне законодавство такого визначення прямо не дає. Воно не зустрічалося і в старому Кримінальному кодексі України. При зверненні до наукових джерел налічено біля 30 визначень категорій "безпека", та похідних від нього "небезпека", "забезпечення", "інформаційна безпека" тощо. При аналізі цих визначень їх сутність зводиться до таких парадигм: стан, суспільні відносини, процес. Виникає питання, як же все таки розуміти ці категорії, якої думки притримуватися? Можна звернутися за аналогією до іншого законодавства України. Але ж у п. 4 ст. 3 КК це прямо заборонено. Можна застосувати положення бланкетності норм кримінального права. Але ж це можливо тільки у випадках, прямо визначених у

диспозиціях статей Особливої частини КК. Постає питання, якщо практики будуть по різному розуміти зазначені категорії (тобто вони будуть викликати різну рефлексію у різних учасників суспільних відносин), то чи можна беззастережно говорити про правильне виконання функцій кримінального законодавства.

Можливий вихід: у ряді Законів України існує відсилання до КК, кримінального законодавства. Наприклад, у Законі "Про захист інформації в автоматизованих системах" (далі Закон), у ст. 17 (Відповідальність за порушення Закону про захист інформації) зазначено, що особи, винні в порушенні порядку і правил захисту оброблюваної в АС інформації, несуть…***кримінальну***…відповідальність згідно з чинним законодавством України. Тобто у цьому Законі (як і у ряді деяких інших Законів України) робиться бланкетна прив'язка до КК. Коли звертаємося до Особливої частини КК - то подібність за змістом таких відносин можна знайти у Розділі XVI (Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж). Але знову виникає питання: зазначений Закон не має узгодженості з КК щодо визначення предмета злочинного посягання: у цих законодавчих актах вживаються різні категорії: у КК – "комп'ютерна інформація", у Законі "інформація в АС". Чи можна їх вважати ідентичними?

Подібна колізія існує і щодо категорій "майно", "власність". Закон України "Про інформацію" визначив нові парадигми цих категорій: інформація, як вид майна і власності. Парадоксально, але до цього часу новий зміст (так як і старий) категорій майна і власності у Законі України "Про власність" не мають свого чіткого визначення. У правовій доктрині вони існують на інтуїтивному рівні. А як відомо, інтуїція у всіх може бути різною в залежності від рівня обізнаності суб'єкта. Виникає необхідність вирішення парадоксу через нові парадигми.

На цьому повернемося знову до розгляду категорії "безпека" у структурі Особливої частини КК. У ній категорія "безпека" є визначною ознакою ряду родових об'єктів. Наприклад: Розділ І. Злочини проти основ національної ***безпеки*** України; Розділ IX. Злочини проти громадської ***безпеки;*** Розділ XX. Злочини проти миру, ***безпеки*** людства та міжнародного порядку та ряд інших.

Категорія "безпека" визначена і в складі окремих статей у інших Розділах Особливої частини КК. Наприклад, у Розділі II. Злочини проти життя та здоров'я особи, у статті 132 (Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби) зазначено це наступним чином "…що є не**безп**ечною для життя людини…". У Розділі V. Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина, сутність категорії "інформаційна безпека" розкривається у ст. 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передається засобами зв'язку або через комп'ютер, а також у ст. 176. Порушення авторських прав і суміжних прав та ст. 182. Порушення недоторканості приватного життя.

Тобто зазначені категорії займають визначне місце у кримінальному праві. Але, як свідчить структура Особливої частини КК, ці категорії не набули означеного місця. Пояснити такий стан можна тим, що вітчизняна теорія кримінального права зупинилася у розвитку свого системного підходу. Системний підхід у традиційній науці кримінального права базується на спрощеному (застарілому) розумінні за моделлю "система – підсистема"; "вид злочину (безпосередній об'єкт) – родовий об'єкт".

На межі правознавства та інформатики виникла нова теорія систем - теорія гіперситсем права. За цією теорією право (у тому числі кримінальне право) розглядається як велика, складна система з підсистемами та субсистемами першого, другого та подальших порядків зі специфічними гіперзв'язками. Адаптація теорії гіперсистем права, як нової парадигми, до потреб науки кримінального права – це питання майбутнього. Серед галузей правознавства теорія гіперсистем права вже набула застосування – у цивільному та інформаційному праві.

На завершення роздумів, для дискусії у правознавстві пропонується наступна теза.

Провідним системоутворюючим об'єктом кримінального права стануть суспільні відносини щодо захисту безпеки, як означного чинника правопорядку, у тому числі інформаційної безпеки. Родовими об'єктами будуть визначені злочини проти безпеки людини (громадянина), злочини проти безпеки суспільства (громадського правопорядку, громадянського миру), злочини проти безпеки держави та злочини проти міжнародної безпеки (міжнародного правопорядку, безпеки людства). Зазначені категорії будуть означеними у такій структурі Особливої частини КК, як (орієнтовно) Книги. Існуючі Розділи Особливої частини будуть систематизовані у статусі підродових (субродових) об'єктів.

Практичне значення такого підходу – чітке окреслення суб'єктно-об'єктних ознак захисту, що визначаються кримінальним законодавством. Організаційно-системне – єднання "математики" кримінального права з юридичною статистикою, правовою інформатикою та кримінологією.

Обґрунтування окремих положень визначених тез знайшло відображення у публікаціях, деякі з них подаються.

Література: 1. Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій. /Камлик М. І., Романюк Б. В., Гавловський В. Д., Хахановський В. Г., Цимбалюк В. С. /за заг. ред. Я. Ю. Кондратьєва. – К. НАВСУ. 2000. 2. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій /Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. /За заг. ред. д. ю. н. Калюжного Р. А. –Запоріжжя: "Просвіта". 2001. 3. Цимбалюк В. С., Гавловський В. Д. Інформаційне право. Навчально-методичний комплекс. К. Інститут економіки управління та господарського права. 1999. 4. Швець М., Гавловський В., Калюжний Р., Цимбалюк В. С Інформаційне законодавство України: концептуальні основи формування. // Право України. 2001. № 7. С. 88 – 81.

УДК 621.391.82

ФОРМАЛІЗАЦІЯ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Олександр Серков
Національний технічний університет «ХПІ»

Анотація: **Узагальнено та формалізовано поняття живучості інформаційних систем, яке базується на позиції загальної теорії систем та теорії множин.**
Summary: **Is generalized and the concept of survivability of information systems is formalized which is based on a position of the general theory of systems and theory of sets.**
Ключові слова: **Живучість, інформаційна система, структурно-функціональне уявлення системи**.

I Вступ

Стрімкий розвиток інформаційних технологій та впровадження їх в усі сфери діяльності суспільства вимагає забезпечення безпеки інформації та інформаційних процесів. Однією із базових складових функцій безпеки, яка відтепер розглядається як одна із загальних задач захисту, є задача забезпечення живучості інформаційних систем. Це обумовлено наявністю загроз, що викликають деструктивні зміни як в інформації, так і в самих інформаційних системах. Таким чином, можливість виникнення порушень у функціонуванні інформаційних систем визначає актуальність проблеми визначення впливу загроз на основні характеристики інформаційних систем та процесів.

Складність побудови інформаційних систем обумовлює їх модельне дослідження з метою визначення основних показників функціонування. В той же час побудова адекватної моделі потребує формалізації процесу забезпечення живучості інформаційних систем та процесів. Однак зараз існує багато підходів до формального опису моделі захисту. У першу чергу слід відзначити теоретичні – ігрові, імовірнісні, детерміновані та графові моделі для аналізу живучості. Найповніше розроблені імовірнісні та детерміновані моделі для аналізу живучості.

Таким чином наявність різноманітних підходів до проблеми забезпечення живучості інформаційних систем [1–3] обумовило необхідність їх узагальнення та створення підходу до їх вирішення з єдиних позицій.

II Постановка завдання

Живучість інформаційної системи не може розглядатися відокремлено від зовнішнього середовища. При цьому під інформаційними системами будемо розуміти динамічні системи, що виконують свої функції на основі використання деякої інформації про ситуації та процеси, які здійснюються як за межами систем, так і у самих системах [4].

Діяльність зовнішнього середовища може бути кваліфікована як бажана, небажана та індиферентна. У найпростішому випадку, коли зовнішнє середовище стаціонарне та випадкове, його дії можливо спрогнозувати. Це дозволяє вжити певних заходів для захисту від небажаних впливів. Для не стаціонарного впливу можливо прогнозування з точки зору найбільш ймовірних дій, їх максимальної потужності. Таким чином небажаний вплив зовнішнього середовища може викликати руйнування на програмному та апаратному рівнях.

Умови, за яких інформаційна система існує та функціонує, описується безліччю вхідних **X** та вихідних **Y** об'єктів. Існування та функціонування інформаційної системи обумовлює реалізацію на безлічі **X** та **Y** деякого відношення $\mathbf{S} \subset \mathbf{X} \times \mathbf{Y}$, причому $\mathbf{S} \in \mathbf{S}^*$, де $\mathbf{S}^*$ – відношення, що реалізується системою. При цьому система має деяку структуру **st** із безлічі можливих структур **St** та набір функцій **f** із безлічі можливих наборів функцій **F.** Сукупність визначеної структури та функції обумовлює реалізацію відповідного